

Noncompliance with new ID theft law could cost businesses

Does your company safely maintain its consumer data? Now is the time to ensure that it does, or suffer the consequences under a recently enacted law that will have a significant impact on Oregon businesses. While compliance with the law may be costly, a failure to comply may cost more.

In the wake of high-profile security breaches and increased concerns over identity theft, Gov. Ted Kulongoski recently signed into law the Oregon Consumer Theft Protection Act. The Department of Consumer and Business Services is charged with administering the new law, and it plans to add an investigator and a hearings officer to its roster to do so. The law takes effect Oct. 1, although some provisions do not apply until Jan. 1.

Many of the details surrounding the law's application will be unclear until the Department of Consumer and Business Services adopts regulations governing its administration. What is clear is that the law's scope is quite broad.

Although it exempts those subject to more stringent federal laws — financial institutions, for example — it otherwise applies to any person or entity possessing data that includes “a consumer's personal information.” A “consumer” is any Oregon resident, and “personal information” is a consumer's name in combination with a Social Security number, driver's license number, passport number, or financial account number and access code.

The law grants significant rights to individuals, including the right to obtain a “security freeze” on one's credit file. For businesses, however, the law creates significant obligations to develop and implement a program to protect consumer information; to provide notice when a security breach occurs; and to abide by the state's authority to investigate and punish violations of the law.

SECURITY COMPLIANCE PROGRAMS

Starting Jan. 1, any person possessing a consumer's “personal information” must have



**GUEST
COLUMN**

Tom
Sondag



**GUEST
COLUMN**

Stephanie
Hendricks

in place a security compliance program providing “reasonable safeguards to protect the security, confidentiality and integrity of the personal information.” Specifically, an adequate security program must provide administrative, technical and physical safeguards:

- Administrative safeguards include identifying security risks, training employees in security practices and procedures, selecting service providers that themselves provide appropriate safeguards — and spell out those safeguards in their contracts — and designating a person to coordinate the security program.

- Technical safeguards include detecting, preventing and responding to system failures, regularly testing systems and procedures, and evaluating risks in the processing, transmission and storage of information.

- Finally, physical safeguards include detecting, preventing and responding to intrusions, preventing unauthorized use of personal information, and destroying information when it's no longer needed.

Notwithstanding the foregoing requirements, the law permits “small businesses” — manufacturing businesses with 200 or fewer employees and all businesses with 50 or fewer employees — to implement practices “appropriate to the size and complexity” of their businesses and to the sensitivity of the personal information they collect.

Nonetheless, caution suggests that a business owner attempt to comply with the law's express requirements.

NOTICE REQUIREMENTS

If a business has a security breach that compromises the security and confidentiality of a consumer's personal information, the consumer must be notified “in the most expeditious time possible.” Such notice may be by letter, e-mail or phone, unless the cost will exceed \$250,000 or the breach affects more than 350,000 con-

sumers — in that event, notice may be published through the media.

PENALTIES FOR NONCOMPLIANCE

The Department of Consumer and Business Services is authorized to enjoin violations of the law, and to impose penalties of up to \$1,000. A separate penalty is imposed for each day a violation continues, but the maximum penalty for any occurrence cannot exceed \$500,000.

In addition, the department may order a business to compensate an individual for injuries caused by a security breach, although it will do so only if it determines that a “private civil action would be so burdensome or expensive as to be impractical.”

Finally, the threat of civil liability is real. Numerous lawsuits have been filed around the country based on the failure of companies to keep private information secure.

While it has previously been difficult to pursue such claims in Oregon courts, the obligations created by the new law arguably change the playing field. And potential lawsuits are not limited to claims by individuals. For example, financial institutions have sued businesses to recover amounts paid in reimbursement of credit card customers whose private data has been compromised.

If nothing else, the new law sounds a warning for all businesses of the potential liabilities that can arise from storing consumer data. Virtually any “breach of security” will have repercussions, and breaches that affect numerous persons will be fodder for class actions.

Although complying with the law will have costs, it's likely to be cheaper than the alternative.

TOM SONDAG is a shareholder at Lane Powell PC, where he specializes in appellate litigation and chairs the Portland office's complex litigation practice group. He can be reached at 503-778-2111 or sondagt@lanepowell.com.

STEPHANIE HENDRICKS, an associate at Lane Powell PC, practices in the area of complex civil and corporate litigation. She can be reached at 503-773-2113 or hendrickss@lanepowell.com.